(19) Europäisches Patentamt / European Patent Office / Office européen des brevets

(11) EP 2 569 904 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
02.12.2020 Bulletin 2020/49

(21) Application number: **10851483.7**

(22) Date of filing: **10.05.2010**

(51) Int Cl.:
H04L 12/437 *(2006.01)* ***H04L 12/46*** *(2006.01)*
H04L 12/28 *(2006.01)*

(86) International application number:
PCT/SE2010/050511

(87) International publication number:
WO 2011/142697 (17.11.2011 Gazette 2011/46)

(54) **A RING NODE, AN ETHERNET RING AND METHODS FOR LOOP PROTECTION IN AN ETHERNET RING**

RINGKNOTEN, ETHERNETRING UND SCHLEIFENSCHUTZVERFAHREN IN EINEM ETHERNETRING

NOEUD D'ANNEAU, ANNEAU ETHERNET ET PROCÉDÉS DE PROTECTION CONTRE LES BOUCLES DANS UN ANNEAU ETHERNET

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

(43) Date of publication of application:
20.03.2013 Bulletin 2013/12

(73) Proprietor: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm (SE)

(72) Inventors:
- **BOS, Juergen**
  50676 Köln (DE)
- **GOUGH, Richard**
  Nottingham
  Nottinghamshire NG12 2NF (GB)
- **THYRESSON, Love**
  S-113 20 Stockholm (SE)
- **VOLKERING, John**
  NL-3481GD Harmelen (NL)

(74) Representative: **Ericsson Patent Development**
Torshamnsgatan 21-23
164 80 Stockholm (SE)

(56) References cited:
EP-A1- 2 086 175 **GB-A- 2 171 880**
US-A1- 2008 285 466 **US-A1- 2009 016 214**
US-A1- 2009 168 647 **US-A1- 2009 168 647**
US-A1- 2010 287 405 **US-A1- 2010 287 405**

- **LEE DOOJEONG ET AL.: 'Efficient ethernet multi-ring protection system' IEEE COMMUNICATIONS MAGAZINE 01 September 2008, XP031570689**
- **DOOJEONG LEE ET AL: "Efficient ethernet multi-ring protection system", DESIGN OF RELIABLE COMMUNICATION NETWORKS, 2009. DRCN 2009. 7TH INTERNATIONAL WORKSHOP ON, IEEE, PISCATAWAY, NJ, USA, 25 October 2009 (2009-10-25), pages 305-311, XP031570689, ISBN: 978-1-4244-5047-3**

EP 2 569 904 B1

Description

Technical field

[0001] The invention relates to Ethernet networks, and in particular to a ring node for loop protection in an Ethernet ring. The invention further relates to an Ethernet ring, and methods for use in the ring node and in the Ethernet ring.

Background

[0002] An Ethernet ring is a collection of ring nodes forming a closed loop whereby each ring node is connected to two adjacent ring nodes via duplex communication links. Fig. 1 illustrates an Ethernet ring 1 comprising seven ring nodes A-G connected to each other via duplex communication links 2.

[0003] A loop of data in the Ethernet ring 1 consumes a lot of resources in the Ethernet ring 1 and is therefore an undesired condition. There is therefore a need for protection against loops in the Ethernet ring 1. The topology of an Ethernet Ring Protection (ERP) network can be a single Ethernet ring or a collection of interconnected Ethernet rings.

[0004] The G.8032 protocol is designed for Ethernet ring topologies and is developed as a standardized alternative to replace the spanning tree protocol (xSTP). It assumes standard 802.1 Q bridges are used and standard 802.3 MAC frames go around the Ethernet ring. G.8032 Ethernet ring nodes generally support standard FDB MAC learning, forwarding, flush behavior and port blocking/unblocking mechanisms.

[0005] The principle of loop prevention within the Ethernet ring 1 is to block one of the ring links 2, either a pre-determined link or a failed link. For example, in a normal state where there is no link failure, as in Fig. 1, one of the ring links 2 is designated as a Ring Protection Link (RPL) 3. The RPL. 3 blocks Ethernet traffic to avoid traffic looping. An RPL 3 blocking is provided by port blocking at both ends of the RPL 3. One of the nodes is called RPL Owner Node 4, e.g. the ring node G, which is also responsible for activating reversion behavior from protected, Manual Switching or Forced Switching conditions. The other node is called RPL Node 5, e.g. the ring node A, which is not responsible for activating reversion behavior. In G.8032 version 1, one end of RPL 3 is blocked for breaking the loop in the normal state. In the draft of G.8032 version 2, both ends of RPL 3 are blocked in a normal state to avoid unnecessary flooding.

[0006] Fig. 2 illustrates an Ethernet Ring Protection (ERP) state. When a link failure occurs, for example, a link 24 between ring node D and ring node E. Ring node D and ring node E block ports 22, 23 for the failed link 24 and send Ring-APS (R-APS) Signal Failure (SF) messages to indicate the link failure. The SF messages are circulated around the Ethernet ring through a Ring APS channel (not shown). When the RPL Owner node G and the RPL node A receive this message, they unblock the ports 4A, 5A to the RPL 3.

[0007] When a link failure is restored, for example, if the link failure between ring node D and ring node E in Fig. 2 disappears, then ring node D and ring node E keep port 22 and port 23 blocked and send out R-APS No Failure message. The messages are circulated around the ring through Ring APS channel. When the RPL Owner node G and RPL node A receive this message, they block the ports 4A, 5A to RPL 3 and send out R-APS Blocking messages. Ring node D and ring node E unblock the port 22 and 23 when they receive the R-APS Blocking messages from ring node G and ring node A. Now the ERP ring is back to the normal state.

[0008] However, Ethernet networks in such ring topologies are not necessarily constructed with the same Ethernet switch hardware for each ring node in the Ethernet ring. For example, a Metro Aggregation Network or a Mobile Backhaul Network may be connected to and be configured to aggregate data traffic from subscribers to Metro Core nodes located in the IP core, e.g. in the Ethernet ring. This aggregation or backhaul network may be built with different Carrier Ethernet technologies, for example, the Metro Aggregation Network may use pure L2 technologies and the Metro Core nodes may use IP/MPLS technologies. Thus, the Metro Core nodes may not be configured or capable to run the G.8032 protocol. This causes problems when connecting the Metro Core nodes to an otherwise G.8032 compliant Ethernet ring and results in long overall service restoration times and lost data traffic for ong periods of time.

[0009] The publication by DOOJEONG LEE ET AL entitled "Efficient Ethernet multi-ring protection system", discloses a protection system for a heterogeneous ring arrangement. The published patent application US 2009/168647 describes an interconnection of a Ethernet protection ring with a backbone network running xSTP protocols. Reconfigurations of the STP network trigger flushing of the forwarding databases of the ring nodes.

Summary

[0010] It is understood by the inventor that it is desirable to achieve Ethernet ring protection (ERP) in Ethernet rings with improved service restoration times.

[0011] The problem is addressed by a first ring node according to independent claim 1 and a method according to independent claim 9. Other embodiments are set out in the dependent claims.

Brief description of the drawings

[0012] The objects, advantages and effects as well as features of the invention will be more readily understood from the following detailed description of exemplary embodiments of the invention when read together with the accompanying drawings, in which:

Fig. 1 illustrates schematically an Ethernet ring.

Fig. 2 illustrates schematically an Ethernet Ring Protection (ERP) state in an Ethernet ring.

Fig. 3 illustrates schematically interworking of a non-G.8032 capable node with an G.8032 Ethernet ring.

Fig. 4 illustrates schematically another interworking of a non-G.8032 capable node with an G.8032 Ethernet ring.

Fig. 5 illustrates schematically interworking of two adjacent G.8032 capable nodes C 53 and E 54 in an G.8032 Ethernet ring with a non-G.8032 capable node 32 according to an embodiment of the invention.

Fig. 6 illustrates schematically interworking of two adjacent G.8032 capable nodes C 53 and E 54 in an G.8032 Ethernet ring with dual non-G.8032 capable nodes 32 according to another embodiment of the invention.

Fig. 7 shows a signalling diagram illustrating a method for handling a single link failure in an G.8032 Ethernet ring comprising a non-G.8032 capable node D 32 according to an embodiment of the invention.

Fig. 8 shows a signalling diagram illustrating a method for handling a single link failure in an G.8032 Ethernet ring comprising a non-G.8032 capable node D 32 according to a further embodiment of the invention.

Fig. 9 shows a signalling diagram illustrating a method for handling initial configuration of a non-G.8032 capable node D 32 in an G.8032 Ethernet ring according to a further embodiment of the invention.

Fig. 10 shows a flowchart of a method according to a further embodiment of the invention.

Detailed description

[0013] Fig. 3 shows schematically an Ethernet ring 31 comprising seven ring nodes A-G connected to each other via duplex communication links. The ring nodes A-C and E-G in the Ethernet ring 31 are G.8032 capable nodes, where the ring node G is the RPL Owner Node 4 and the ring node A is the RPL Node 5. However, in the Ethernet ring 31, a non-G.8032 capable node 32, i.e. ring node D, is connected to adjacent G.8032 capable ring nodes C and E and thus forms part of the otherwise G.8032 compliant Ethernet ring 31.

[0014] In order enable the Ethernet ring protection (ERP) according to the Ethernet ring protection protocol standard G.8032 in the Ethernet ring 31, one interworking alternative arrangement is shown in Fig. 3, where the adjacent G.8032 capable ring nodes C and E are arranged to tunnel the VLAN that comprises the R-APS messages 33 according to the Ethernet ring protection protocol standard G.8032 through the non-G.8032 capable node D 32.

[0015] However, as previously mentioned above, in an G.8032 capable Ethernet ring and upon the occurence of a link failure or recovery event, Ring-APS (R-APS) Signal Failure (SF) messages will be circulated around the Ethernet ring to indicate the link failure or recovery. In order to rebuild the filtering databases (FDBs) in each of the ring nodes due to the resulting ring topology change, the SF messages are also arranged to to activate all ring nodes to "flush" their FDBs so that all FDB entries are cleared. It should be noted that the FDB entries here refers only to the MAC addresses learnt on the ERP ring ports in the ring nodes and not on other ports in the ring nodes. The FDB MAC learning process will then rebuild the FDBs with new FDB entries as all data traffic frames, now with unknown destination addresses, subsequently will be flooded, i.e. broadcasted, throughout the G.8032 capable Ethernet ring.

[0016] However, if there is a ring node D 32 in the G.8032 Ethernet ring 31 which is not configured to perform ERP according to the ERP protocol standard G.8032, the non-G.8032 capable node D 32 will not flush its FDB in case of a link failure or recovery event. The non-G.8032 capable node D 32 will therefore comprise erroneous FDB entries in its FDB which may take the FDB MAC learning process a long time to correct. In a worst case, data traffic can consequently be lost up to a time period corresponding to the FDB MAC address aging time, which is typically in a range of 5 minutes. Thus, while the physical layer in the Ethernet ring 31 may be protected within 50 ms as indicated by the ERP protocol standard G.8032, the service layer responsible for the Ethernet data traffic will only be restored with the speed of FDB MAC learning process and is also well dependent on the available bandwidth for the flooding of the data traffic frames. Consequently, the result is long service restoration time of the service layer responsible for the Ethernet data traffic in the Ethernet ring 31 upon a link failure or recovery event. This is particularly critical for sensitive data traffic applications such as, for example, for real-time gaming applications, etc.

[0017] In order to overcome the problems described above, another interworking alternative arrangement is shown by the Ethernet ring 41 in Fig. 4. Here, a redundant G.8032 capable ring node 11 42 has been provided in the Ethernet ring 41 to act as an intermediate ring node between the non-G.8032 capable node D 32 and the now fully G.8032 compliant Ethernet ring 41. The non-G.8032 capable node D 32 may be connected redundantly via a Link Aggregation Group 43 (LAG) to the G.8032 capable ring node H 42 in the Ethernet ring 41. However, in case of failures of the LAG 43, this interworking alternative arrangement suffers from the disadvantage of having even longer convergence and service restoration times than the previous alternative. This arrangement also incur additional implementation costs since it requires two ring nodes instead of one ring node to be deployed in connecting the non-G.8032 capable node D 32 to the Ethernet ring 41, and additional interfaces have to be provided in order to ba able to realize the connection. Furthermore, often the implementation of a LAG 43 does not guarantee full bandwidth utilization since the data traffic distribution algorithms in the ring node do not always lead to a well balanced usage of the single LAG 43 constituents.

[0018] Fig. 5 shows schematically the interworking of two adjacent G.8032 capable nodes C 53 and E 54 in an Ethernet ring 51 with a non-G.8032 capable node 32 according to an embodiment of the invention. As in the alternative interworking arrangement described in relation to Fig. 3, the two adjacent G.8032 capable nodes C 53 and E 54 in the Ethernet ring 51 may here be arranged to tunnel the VLAN that comprises the R-APS messages 55 according to the Ethernet ring protection protocol standard G.8032 through the non-G.8032 capable node D 32.

[0019] Upon detecting a link failure or recovery event in the Ethernet ring 51, the two adjacent G.8032 capable nodes C 53 and E 54 may decide in accordance with the ERP protocol standard to perform a flush operation of its filtering database (FDB).

[0020] In response to this decision to perform the flush operation and according to an embodiment of the invention, the two adjacent G.8032 capable nodes C 53 and E 54 may be configured to also send a message 56 to the non-G.8032 capable node D 32. The message may be operable to cause the non-G.8032 capable node D 32 to also perform a flush operation of its filtering database (FDB). The flush operation in the non-G.8032 capable node D 32 then removes all prior FDB entries from the FDB in the non-G.8032 capable node D 32, except for the FDB entries for the ports on which it received the messages from each of the two adjacent G.8032 capable nodes C 53 and E 54. It should be noted that when referring to FDB entries only the MAC addresses learnt on the ERP ring ports are intended and not on other ports in the ring nodes.

[0021] In case the non-G.8032 capable node D 32 is configured to perform ERP according to the Spanning Tree Protocol (STP), the message 56 may be a Spanning Tree Protocol Topology Change Notification (STP TCN). In case the non-G.8032 capable node D 32 is configured to perform ERP according to the Rapid Spanning Tree Protocol (RSTP), the message 56 may be a Rapid Spanning Tree Protocol Topology Change Notification (RSTP TCN). The messages 56 may be sent by the two adjacent G.8032 capable nodes C 53 and E 54 in the Ethernet ring 51 using the internal Network-Network-Interface (I-NNI). Thus, the messages 56 will force the non-G.8032 capable node D 32 to flush its filtering database (FDB) twice, once for each message 56 received from each of the two adjacent G.8032 capable nodes C 53 and E 54 in the Ethernet ring 51. This ensures that the FDB is flushed on both ring ports in the non-G.8032 capable node D 32, that is, the message 56 received from the left adjacent G.8032 capable node C 53 on the left ring port in the non-G.8032 capable node D 32 invokes a flush operation for the right ring ports, while the message 56 received from the right adjacent G.8032 capable node E 54 on the right ring port in the non-G.8032 capable node D 32 invokes a flush operation for the left ring ports. The signalling of each of the two adjacent G.8032 capable nodes C 53 and E 54 are described in more detail below in relation to Fig. 7.

[0022] By having each of the two adjacent G.8032 capable nodes C 53 and E 54 being arranged to translate events that trigger an FDB flush operation in each of the two adjacent G.8032 capable nodes C 53 and E 54 to an event which will trigger a FDB flush operation in the non-G.8032 capable node D 32, the service restoration times of the Ethernet ring 51 may be kept at substantially the same level as in a pure G.8032 capable Ethernet ring wherein all ring nodes A-G performs ERP according to the ERP protocol standard G.8032. This because the FDB in the non-G.8032 capable node D 32 will now also be flushed as the FDBs in the two adjacent G.8032 capable nodes C 53 and E 54 are flushed in accordance with the ERP protocol standard G.8032. This will minimize the time it will take the FDB MAC learning process in both the non-G.8032 capable node D 32 and the G.8032 capable nodes A-C and E-G to rebuild all the FDBs with new FDB entries according to the new Ethernet ring topology. This because all data traffic frames received at the non-G.8032 capable node D 32 and the G.8032 capable nodes A-C and E-G now being broadcasted throughout the Ethernet ring 51 due to the fact they comprise unknown addresses, will directly start to populate the FDBs with new FDB entries according to the new Ethernet ring topology. As a consequence, the service restoration time of the service layer responsible for the Ethernet data traffic in the Ethernet ring 51 will be minimized. Furthermore, due to the fact that there is no risk of having old and erroneous FDB entries in the FDBs, potential data traffic losses is further eliminated.

[0023] The two adjacent G.8032 capable nodes C 53 and E 54 may further be configured to react to configuration messages sent by the non-G.8032 capable node D 32 if the non-G.8032 capable node D 32 is running ERP according to another ERP protocol standard. This is described in more detail below in relation to Fig. 8.

[0024] Also, since the ITU-T G.8032: Ethernet ring protection switching standard document also implements FDB flush optimizations to avoid these when unnecessary, the two adjacent G.8032 capable nodes C 53 and E 54 may also be configured to correlate the sending of the messages 56 in accordance with these flush optimisations.

[0025] Furthermore, in order to detect link failure or recovery events that can not be discovered physically between two adjacent G.8032 capable nodes C 53 and E 54 using the VLAN tunnel, the links between the two adjacent G.8032 capable nodes C 53 and E 54 and the non-G.8032 capable node D 32 may additionally be supervised by Ethernet Continuity Check Messages (CCM) in accordance with the IEEE 802.1ag Connectivity Fault Management standard document. By defining the two adjacent G.8032 capable nodes C 53 and E 54 and the non-G.8032 capable node D 32 as Maintence End Points (MEP) on all links that are supervised by Ethernet Continuity Check Messages (CCM), detection of link failure or recovery events that can not be discovered physically between two adjacent G.8032 capable nodes C 53 and E 54 using the VLAN tunnel is enabled. Preferably, in such a configuration, all ring nodes A-G in the Ethernet ring 51 are defined as Maintence End Points (MEP) and all links in the Ethernet ring 51 supervised by Ethernet Continuity Check Messages (CCM).

[0026] Fig. 6 shows schematically the interworking of two adjacent G.8032 capable nodes C 53 and E 54 in an Ethernet ring 61 with dual non-G.8032 capable nodes 32, i.e. ring nodes D1 and D2, according to another embodiment of the invention. The dual non-G.8032 capable nodes D1, D2 32 may be provided in order to have redundancy towards an Metro aggregation or backhaul network 69 being connected to the Ethernet ring 61 through the dual non-G.8032 capable nodes D1, D2 32. Here, the two adjacent G.8032 capable nodes C 53 and E 54 in the Ethernet ring 61 may also be arranged to tunnel the VLAN that comprises the R-APS messages 55 according to the Ethernet ring protection protocol standard G.8032 through both of the non-G.8032 capable nodes D1, D2 32.

[0027] In this embodiment, it needs to be guaranteed that the logical connection between the two adjacent G.8032 capable nodes C 53 and E 54, i.e. the VLAN transporting the R-APS messages, continuously exists. Resiliency measures that ensure the connectivity between dual non-G.8032 capable nodes D1, D2 32 may therefore be provided using, for example, MPLS or STP technologies.

[0028] In the previous embodiment, the non-G.8032 capable node D 32 is forced to flush its filtering database (FDB) once for each message 56 received from each of the two adjacent G.8032 capable nodes C 53 and E 54 in the Ethernet ring 51. In this embodiment, the non-G.8032 capable nodes D1 and D2 32 will only receive one message 56 from its adjacent G.8032 capable nodes C 53 and E 54, respectively. However, for example, if the nodes D1 and D2 are configured to perform ERP according to STP, one of the nodes D1 and D2 will become the root bridge and the other one a non-root bridge. Assuming that D1 is determined to be the root bridge, the root node D1 will receive the TCN message 56 from its left adjacent G.8032 capable node C 53 on its left ring port which invokes a flush operation for its right ring ports. This will also result in that the root node D1 sends a TCN message to the non-root node D2. The non-root node D2 will thus receive one TCN message from the root node D1 and one TCN message 56 from its right adjacent G.8032 capable node E 54 resulting in a flush operation on both right and left ring ports. Additionally, the non-root node D2 may forward the TCN received from its right adjacent G.8032 capable node E 54 to its root node D1. The root node D1 will thus also receive a TCN message on its right ring port which invokes a flush operation for its left ring ports. This ensures that the FDB is flushed on both ring ports in both of the non-G.8032 capable nodes D1 and D2 32.

[0029] Fig. 7 shows a signalling diagram illustrating a method for handling a single link failure in an G.8032 Ethernet ring comprising a non-G.8032 capable node D 32 according to an embodiment of the invention. The signalling diagram in Fig. 7 may be compared with the signalling diagram shown in Figure 1V-1/G.8032/Y.1344-Single link failure in the ITU-T G.8032; Ethernet ring protection switching standard document.

[0030] In step S1, the Ethernet ring 51 operates in a normal state where no link failure has occured. The RPL blocking is provided by R-APS channel or port blocking at both ends of the RPL, i.e. in both the RPL Owner Node G and the RPL Node A.

[0031] In step S2, a single link failure occurs between the ring nodes B and C.

[0032] In step S3, the ring nodes B and C detects the link failure event and after respecting the holdoff time, blocks the failed R-APS channel or port.

[0033] In step S4, the ring nodes B and C periodically send Signal Failure (SF) messages, on both ring ports, as long as the single link failure persists. In Fig. 7, this is shown by the filled circles indicating the source of the SF messages. Furthermore, in response to the detected link failure event in step S3, the ring nodes B and C may decide to flush its filtering database (FDB).

[0034] As indicated by the dashed area 71 in Fig. 7 and according to an embodiment of the invention, since the ring node C is an adjacent G.8032 capable ring node C 53 connected to the non-G.8032 capable ring node D 32 it sends, in response to its decision to flush its FDB, a message to the non-G.8032 capable ring node D 32 which is operable to cause the non-G.8032 capable ring node D 32 to also flush its FDB. If, for example, the non-G.8032 capable ring node D 32 is configured to perform ERP according to the STP protocol, the message may be a STP TCN message as shown in Fig. 7. Upon receiving the STP TCN message from the G.8032 capable ring node C 53, the non-G.8032 capable ring node D 32 will flush its FDB on all ports paticipating in the STP domain except for the port where it received the STP TCN message, i.e. a ring port in the direction of the G.8032 capable ring node C 53. This is standard behaviour of a STP root bridge as described in IEEE 802.1D MAC Bridges.

[0035] Upon receiving the SF message and in response to its decision to flush its FDB, the ring node E being the G.8032 capable ring node E 54 adjacent to a non-G.8032 capable ring node D 32 also sends a message, e.g. a STP TCN message, to the non-G.8032 capable ring node D 32 which is operable to cause the non-G.8032 capable ring node D 32 to flush its FDB. Upon receiving the STP TCN message from the G.8032 capable ring node E 54, the non-G.8032 capable ring node D 32 will flush its FDB on all ports paticipating in the STP domain except for the port where it received the STP TCN message, i.e. a ring port in the direction of the G.8032 capable ring node E 54.

[0036] In step S5, the RPL Owner Node G and the RPL Node A unblocks the RPL at both ends and flushes their FDBs.

[0037] In step S6, the Ethernet ring 51 operates in a stable protection state where SF messages are periodically sent by the ring nodes B and C, on both ring ports, as long as the single link failure persists. The periodical SF messages do not trigger any further action in neither the ring nodes A-B, E-G nor in the adjacent G.8032 capable ring nodes C 53 and E 54.

[0038] It should be noted that although the exemplary method above is described for single link failure event, the method may also similarly be applied for other link failure events or recovery events. For example, in case of a single link failure recovery event, the flushing of the FDBs in the adjacent G.8032 capable ring nodes C 53 and E 54 may be triggered by NR RB (No Request, Ring Blocked) messages in case the non-G.8032 capable ring node D 32, for example, is configured to perform ERP according to the STP protocol. Thus, the adjacent G.8032 capable ring nodes C 53 and E 54 may upon receiving the NR RB message and in response to its decision to flush its FDB, send a message, e.g. a STP TGN message, to the non-G.8032 capable ring node D 32 which is operable to cause the non-G.8032 capable ring node D 32 to flush its FDB. This signalling may be compared with the signalling diagram shown in Figure IV-3/G.8032/Y.1344- Single link failure recovery (Non-Revertive operation) in the ITU-T G.8032: Ethernet ring protection switching standard document.

[0039] Other link failure events that may lead to the flushing of the FDBs in the ring nodes A-B, E-G and the adjacent G.8032 capable ring nodes C 53 and E 54 and thus for which the method method described above may be implemented, may include single unidirectional link failures, RPL link failures, etc.

[0040] Fig. 8 shows a signalling diagram illustrating a method for handling a single link failure in an G.8032 Ethernet ring comprising a non-G.8032 capable node D 32 according to an embodiment of the invention. Here, the single link failure occurs in between the adjacent G.8032 capable ring node C 53 and the non-G.8032 capable node D 32.

[0041] In step S11, the Ethernet ring 51 operates in a normal state where no link failure has occured. The RPL blocking is provided by R-APS channel or port blocking at both ends of the RPL, i.e. in both the RPL Owner Node G and the RPL Node A.

[0042] In step S12, a single link failure occurs between the adjacent G.8032 capable ring node C 53 and the non-G.8032 capable node D 32.

[0043] In step S13, the adjacent G.8032 capable ring node C 53 detects the link failure event, e.g. a physical link loss condition, and after respecting the holdoff time, blocks the failed R-APS channel or port. The non-G.8032 capable node D 32 also detects the link failure event and after respecting the holdoff time, blocks the failed port. In case the non-G.8032 capable node D 32 is configured to run STP, the non-G.8032 capable node D 32 assumes that it is the root bridge and will consequently invoke a FDB flush operation for all ports participating in the STP domain except for the port for which it detected the link failure event and send a TCN message to the adjacent G.8032 capable ring node E 54. Again, this is standard behaviour of a STP root bridge as described in IEEE 802.1D MAC Bridges. The TCN message may be ignored by the adjacent G.8032 capable ring node E 54.

[0044] In step S14, the adjacent G.8032 capable ring node C 53 periodically send Signal Failure (SF) messages, on both ring ports, as long as the single link failure persists. In Fig. 8, this is shown by the filled circle indicating the source of the SF messages. Furthermore, in response to the detected link failure event in step S13, the adjacent G.8032 capable ring node C 53 may decide to flush its filtering database (FDB).

[0045] As indicated by the dashed areas 81 in Fig. 8 and according to an embodiment of the invention, since the ring node C is the adjacent G.8032 capable ring node C 53 connected to the non-G.8032 capable ring node D 32 it will try to send, in response to its decision to flush its FDB, a message to the non-G.8032 capable ring node D 32 which is operable to cause the non-G.8032 capable ring node D 32 to also flush its FDB. However, due to the link failure event, the message will not reach the non-G.8032 capable ring node D 32. Upon receiving the SF message from the ring node B, the RPL Owner Node G and the RPL Node A unblocks the RPL at both ends and flushes their FDBs.

[0046] In step S15, upon receiving the SF message and in response to its decision to flush its FDB, the ring node E being the G.8032 capable ring node E 54 adjacent to the non-G.8032 capable ring node D 32 will also try to send a message, e.g. a STP TCN message, to the non-G.8032 capable ring node D 32 which is operable to cause the non-G.8032 capable ring node D 32 to flush its FDB. Contrary to the previous message, this message will reach the non-G.8032 capable ring node D 32 since there is no link failure between the non-G.8032 capable ring node D 32 and the adjacent G.8032 capable ring node E 54. Upon receiving the STP TCN message from the adjacent G.8032 capable ring node E 54, the non-G.8032 capable ring node D 32 will flush its FDB on all ports participating in the STP domain except for the port where it received the STP TCN message, i.e. a ring port in the direction of the G.8032 capable ring node E 54. In our case, however, this FDB flush operation will not take effect since the ring port in the direction of the adjacent G.8032 capable ring node C 53 is anyhow not in operation. It should also be noted that the adjacent G.8032 capable ring node E 54 may keep sending SF messages towards the adjacent G.8032 capable ring node C 53, but the non-G.8032 capable ring node D 32 is not going to be able to pass the SF messages on the adjacent G.8032 capable ring node C 53 due to the single link failure.

[0047] In step S16, the Ethernet ring 51 operates in a stable protection state where SF messages are periodically sent by the adjacent G.8032 capable ring node C 53, on both ring ports, as long as the single link failure persists. The periodical SF messages do not trigger any further action in neither the ring nodes A-B, E-G nor in the adjacent G.8032 capable ring nodes C 53 and E 54.

[0048] It should be noted that although the exemplary method above is described for a single link failure event, the method may also similarly be applied for other link failure events or recovery events as described in relation to the previous embodiment.

[0049] Fig. 9 shows a signalling diagram illustrating a method for handling initial configuration of a non-G.8032 capable node D 32 in an G.8032 Ethernet ring according to an embodiment of the invention. If, for example, the non-G.8032 capable node D 32 is configured perform ERP according to the STP protocol, the non-G.8032 capable node D 32 will assume that it is placed in an Ethernet ring implementing the STP protocol. This will prompt the following initial behaviour of the MAC bridges in the non-G.8032 capable node D 32.

[0050] As the ring node D is turned on, configuration BPDU (Bridge Protocol Data Unit) messages are sent by the ring node D through every connected port at a regular time intervals, e.g. using the Hello Timer with a default timing of every 2 seconds. At start up, every ring node configured to perform ERP according to the STP protocol, such as, the ring node D, believes itself as being the root of the tree, and hence the ring node D will set the Root Identifier to the value of its own Bridge Identifier in the configuration BPDU messages it transmits.

[0051] Normally, when a neighboring ring node configured to perform ERP according to the STP protocol receives this configuration BPDU message, the neighboring ring node compares the received configuration BPDU message with the best BPDU it has. If the neighboring ring node concludes that the new BPDU is better, it will use the sending ring node D as the root and propagate the configuration BPDU messages to other neighboring ring nodes. Otherwise, if the neighboring ring node does not receive any configuration BPDU messages with a better BPDU, it will keep sending configuration BPDU messages assuming itself or the currently best BPDU to be the root bridge.

[0052] According to an embodiment of the invention, the adjacent G.8032 capable ring nodes C 53 and E 54 may therefore be arranged to react on these configuration messages such that the ring node D believes it to be the root bridge an Ethernet ring implementing the STP protocol. As indicated in Fig. 9, this may be performed by the adjacent G.8032 capable ring nodes C 53 and E 54 by simply stopping or discarding the received STP configuration BDU messages from the ring node D. The stopping or discarding of the received STP configuration BDU messages from the ring node D may be performed by existing message filters in the adjacent G.8032 capable ring nodes C 53 and E 54, e.g. using ACLs (Access Control Lists), or by a modification of the software present in the the adjacent G.8032 capable ring nodes C 53 and E 54. Thus, this embodiment describes enhanced behaviour in the adjacent G.8032 capable ring nodes C 53 and E 54 to interwork with a non-G.8032 capable node D 32 running STP during initial setup.

[0053] Furthermore, to interwork with a non-G.8032 capable node D 32 running RSTP, the adjacent G.8032 capable ring nodes C 53 and E 54 additionally needs to react to RSTP BPDU Proposal messages during the root bridge selection phase in the intial setup of RSTP. However, since all ring nodes running RSTP are backward compatible with ring nodes running STP, when implemented according to the IEEE 802. 1D MAC Bridges standard document, and the adjacent G.8032 capable ring nodes C 53 and E 54 easily may be modified to respond in accordance with specific implementations, the interworking with RSTP is not described in any further detail herein.

[0054] Fig. 10 shows a flowchart of a method for handling link failure or recovery events in the adjacent G.8032 capable ring nodes C 53 and E 54 according to a further embodiment of the invention.

[0055] In step S301, the adjacent G.8032 capable ring nodes C 53 and E 54 may be configured to detect a link failure or recovery event. In step S102, the adjacent G.8032 capable ring nodes C 53 and E 54 may decide to perform a flush operation of its FDB in response to the link failure or recovery event detected in step S91. In step S103, the adjacent G.8032 capable ring nodes C 53 and E 54 may be configured to send a message, in response to the decision to perform the flush operation of its FDB, which is operable to cause another network node, e.g. the non-G.8032 capable ring node D 32 or the non-G.8032 capable ring nodes D1 and D2 32, to perform a flush operation of its FDB.

[0056] Although the invention is mainly described above in relation to specific Ethernet ring protection protocol standards, such as, the Ethernet ring protection protocol standards G.8032, STP and RTSP, it should be noted that this is made for illustrative purposes and that other combinations of existing or developing Ethernet ring protection protocol standards may also benefit from the advantages of the invention in a similar manner.

[0057] The description above is of the best mode presently contemplated for practising the present invention. The description is not intended to be taken in a limiting sense, but is made merely for the purpose of describing the general principles of the invention. The scope of the present invention should only be ascertained with reference to the issued claims.

Claims

1. A first ring node (53) arranged to protect against loops in an Ethernet ring (51, 61) by performing Ethernet Ring Protection, ERP, according to an ERP protocol standard, the first ring node (53) being located directly adjacent to at least one second ring node (32) in the Ethernet ring (51, 61), wherein the at least one second ring node (32) is not configured to perform ERP according to the same ERP protocol standard, **characterized in that**
the first ring node (53) is configured to, upon detection of a link failure event or a recovery event in the Ethernet ring (51, 61) resulting in a flush operation of a filtering database, FDB, in the first ring node (53) in accordance with the ERP protocol standard, send a message to the at least one second ring node (32), wherein the message is operable to cause said at least one second ring node (32) to perform a flush operation of an FDB in the at least one second ring node (32).

2. The first ring node (53) according to claim 1, wherein the first ring node (53) is configured to be communicatively connected with a third ring node (54) in the Ethernet ring (51, 61) by tunneling a VLAN used by the ERP protocol standard through the at least one second ring node (32), wherein said third ring node (54) in the Ethernet ring (51, 61) is configured to perform ERP according to the same ERP protocol standard as the first ring node (53).

3. The first ring node (53) according to claim 1 or 2, wherein the at least one second ring node (32) in the Ethernet ring (51, 61) is configured to perform ERP according to another ERP protocol standard.

4. The first ring node (53) according to claim 3, wherein the first ring node (53) is further configured to react to configuration messages sent by the at least one second ring node (32) in the Ethernet ring (51, 61) according to the another ERP protocol standard such that standard operations of ERP, according to the another ERP protocol standard, in the at least one second ring node (32) are not disrupted.

5. The first ring node (53) according to any one of the claims 1-4, wherein the ERP protocol standard for the first ring node (53) is ITU-T G.8032 ERP switching protocol, and the another ERP protocol standard for the at least one second ring node (32) is Spanning Tree Protocol, STP, or Rapid Spanning Tree Protocol, RSTP.

6. The first ring node (53) according to claim 5, wherein, in case the another ERP protocol standard is the RSTP, the first ring node (53) is further configured to respond to the configuration messages sent by the at least one second ring node (32) in the Ethernet ring (51, 61) during the initial setup of the RSTP.

7. The first ring node (53) according to any one of the claims 5-6, wherein the message comprises a Spanning Tree Protocol Topology Change Notification, STP TCN, or a Rapid Spanning Tree Protocol Topology Change Notification, RSTP TCN, and wherein the message is sent by the first ring node (53) to the at least one second ring node (32) using Internal Network-Network-Interface, I-NNI.

8. The first ring node (53) according to any one of the claims 1-7, wherein link failure events or recovery events occuring between the first ring node (53) and the at least one second ring node (32) in the Ethernet ring (51, 61) are additionally supervised by Ethernet Continuity Check Messages, CCM, in accordance with IEEE 802.1 ag Connectivity Fault Management standard protocol.

9. A method for use in a first ring node (53) to protect against loops in an Ethernet ring (51, 61) by performing Ethernet Ring Protection, ERP, according to an ERP protocol standard, the first ring node (53) being located directly adjacent to at least one second ring node (32) in the Ethernet ring (51, 61), wherein the at least one second ring node (32) is not configured to perform ERP according to the same ERP protocol standard, the method comprising the steps of:

detecting a link failure event or a recovery event in the Ethernet ring (51, 61) according to the ERP protocol standard;
deciding to perform a flush operation of a filtering database, FDB, in the first ring node (53) in response to the detected link failure event or the detected recovery event, said method being **characterized by** further comprising the step of:
in response to the decision to perform the flush operation, sending a message to the at least one second ring node (32), wherein the message is operable to cause said at least one second ring node (32) to perform a flush operation of an FDB in the at least one second ring node (32).

10. The method according to claim 9, further comprising the step of:
reacting, wherein the at least one second ring node (32) in the Ethernet ring (51, 61) is configured to perform ERP according to another ERP protocol standard, to configuration messages sent by the at least one second ring node (32) in the Ethernet ring (51, 61) such that standard operations of ERP, according

to the another ERP protocol standard, in the at least one second ring node (32) are not disrupted.

11. The method according to claim 10, further comprising the step of:
responding, in case the another ERP protocol standard is Rapid Spanning Tree Protocol, RSTP, to the configuration messages sent by the at least one second ring node (32) in the Ethernet ring (51, 61) during the initial setup of the RSTP.

12. An Ethernet ring (51, 61) comprising a first ring node (53) according to claim 1 and at least one third ring node (54) arranged to protect against said loops in the Ethernet ring (51, 61) by performing said ERP according to said ERP protocol standard, **characterized in that**
the at least one third ring node (54) that is located directly adjacent to the at least one second ring node (32) in the Ethernet ring (51, 61) is configured to, upon the detection of the link failure event or the recovery event in the Ethernet ring (51, 61) resulting in a flush operation of FDBs in the at least one third ring node (54) in accordance with the ERP protocol standard, send a message to said at least one second ring node (32), wherein the message sent by the at least one third ring node (54) is operable to cause said at least one second ring node (32) to perform a flush operation of the FDB in the at least one second ring node (32).

13. The Ethernet ring (51, 61) according to claim 12, wherein, in case the at least one second ring node (32) is configured to perform ERP according to another ERP protocol standard and comprises more than one ring node (D1, D2), resilience measures for a connectivity between the more than one ring node (D1, D2) are provided.

14. A broadband communications network comprising a first ring node (53) according to claim 1, and/or an Ethernet ring (51, 61) according to claim 12.

15. A method, for use in an Ethernet ring (51, 61), according to claim 9, the Ethernet ring (51, 61) further comprising at least one third ring node (54) arranged to protect against said loops in the Ethernet ring (51, 61) by performing said ERP according to said ERP protocol standard, the method comprising the steps of:
deciding to perform a flush operation of an FDB in the at least one third ring node (54) in response to the detected link failure event or the detected recovery event, the method being **characterized by** further comprising the step of:
in response to the decision to perform the flush operation of said FDB in said at least one third ring node (54), sending a message, from the at least one third ring node (54) that is located directly adjacent to the at least one second ring node (32) in the Ethernet ring (51, 61), to the at least one second ring node (32), wherein the message sent by said at least third ring node (54) is operable to cause said at least one second ring node (32) to perform a flush operation of said FDB in the at least one second ring node (32).

Patentansprüche

1. Erster Ringknoten (53), der zum Schutz gegen Schleifen in einem Ethernetring (51, 61) durch Durchführen eines Ethernetringschutzes (Ethernet Ring Protection - ERP) nach einem ERP-Protokollstandard eingerichtet ist, wobei der erste Ringknoten (53) sich unmittelbar benachbart zu mindestens einem zweiten Ringknoten (32) in dem Ethernetring (51, 61) befindet, wobei der mindestens eine zweite Ringknoten (32) nicht konfiguriert ist, um einen ERP nach demselben ERP-Protokollstandard durchzuführen, **dadurch gekennzeichnet, dass** der erste Ringknoten (53) konfiguriert ist, um bei Erkennen eines Verbindungsfehlerereignisses oder eines Wiederherstellungsereignisses in dem Ethernetring (51, 61), das zu einer Leerungsoperation einer Filterdatenbank (FDB) in dem ersten Ringknoten (53) nach dem ERP-Protokollstandard führt, eine Nachricht an den mindestens einen zweiten Ringknoten (32) zu senden, wobei die Nachricht so betreibbar ist, dass sie den mindestens einen zweiten Ringknoten (32) veranlasst, eine Leerungsoperation einer FDB in dem mindestens einen zweiten Ringknoten (32) durchzuführen.

2. Erster Ringknoten (53) nach Anspruch 1, wobei der erste Ringknoten (53) konfiguriert ist, um durch Tunneln eines von dem ERP-Protokollstandard verwendeten VLAN über den mindestens einen zweiten Ringknoten (32) kommunikativ mit einem dritten Ringknoten (54) in dem Ethernetring (51, 61) verbunden zu sein, wobei der dritte Ringknoten (54) in dem Ethernetring (51, 61) so konfiguriert ist, dass er einen ERP nach demselben ERP-Protokollstandard wie der erste Ringknoten (53) durchführt.

3. Erster Ringknoten (53) nach Anspruch 1 oder 2, wobei der mindestens eine zweite Ringknoten (32) in dem Ethernetring (51, 61) konfiguriert ist, um einen ERP nach einem anderen ERP-Protokollstandard durchzuführen.

4. Erster Ringknoten (53) nach Anspruch 3, wobei der erste Ringknoten (53) ferner konfiguriert ist, um auf Konfigurationsnachrichten, die von dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) nach dem anderen ERP-Protokollstandard gesendet werden, zu reagieren, sodass Standardoperationen des ERP nach dem anderen ERP-Protokollstandard in dem mindestens einen zweiten Ringknoten (32) nicht gestört werden.

5. Erster Ringknoten (53) nach einem der Ansprüche 1-4, wobei der ERP-Protokollstandard für den ersten Ringknoten (53) das ERP-Vermittlungsprotokoll ITU-T G.8032 ist und der andere ERP-Protokollstandard für den mindestens einen zweiten Ringknoten (32) Spanning-Tree-Protokoll (STP) oder Rapid-Spanning-Tree-Protokoll (RSTP) ist.

6. Erster Ringknoten (53) nach Anspruch 5, wobei, falls der andere ERP-Protokollstandard das RSTP ist, der erste Ringknoten (53) ferner konfiguriert ist, um auf die Konfigurationsnachrichten zu antworten, die von dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) während der Ersteinrichtung des RSTP gesendet werden.

7. Erster Ringknoten (53) nach einem der Ansprüche 5-6, wobei die Nachricht eine Spanning-Tree-Protokoll-Topologie-Änderungsbenachrichtigung (Spanning Tree Protocol Topology Change Notification - STP TCN) oder eine Rapid-Spanning-Tree-Protokoll-Topologie-Änderungsbenachrichtigung (Spanning Tree Protocol Topology Change Notification - RSTP TCN) umfasst und wobei die Nachricht durch den ersten Ringknoten (53) unter Verwendung einer internen Netzwerk-zu-Netzwerk-Schnittstelle (Internal Network-Network-Interface - I-NNI) an den mindestens einen zweiten Ringknoten (32) gesendet wird.

8. Erster Ringknoten (53) nach einem der Ansprüche 1-7, wobei Verbindungsfehlerereignisse oder Wiederherstellungsereignisse zwischen dem ersten Ringknoten (53) und dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) zusätzlich durch Durchgangsprüfungsnachrichten (Continuity Check Messages - CCM) des Ethernets nach dem Konnektivitätsfehlermanagement-Standardprotokoll IEEE 802.1 ag überwacht werden.

9. Verfahren zur Verwendung in einem ersten Ringknoten (53) zum Schutz gegen Schleifen in einem Ethernetring (51, 61) durch Durchführen eines Etherneringschutzes (ERP) nach einem ERP-Protokollstandard, wobei der erste Ringknoten (53) sich unmittelbar benachbart zu dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) befindet, wobei der mindestens eine zweite Ringknoten (32) nicht konfiguriert ist, um einen ERP nach demselben ERP-Protokollstandard durchzuführen, wobei das Verfahren die folgenden Schritte umfasst:

Erkennen eines Verbindungsfehlerereignisses oder eines Wiederherstellungsereignisses in dem Ethernetring (51, 61) nach dem ERP-Protokollstandard;

Entscheiden, eine Leerungsoperation einer Filterdatenbank (FDB) in dem ersten Ringknoten (53) als Reaktion auf das erkannte Verbindungsfehlerereignis oder das erkannte Wiederherstellungsereignis durchzuführen, wobei das Verfahren **dadurch gekennzeichnet ist, dass** es ferner den folgenden Schritt umfasst:

als Reaktion auf die Entscheidung, die Leerungsoperation durchzuführen, Senden einer Nachricht an den mindestens einen zweiten Ringknoten (32), wobei die Nachricht so betreibbar ist, dass sie den mindestens einen zweiten Ringknoten (32) veranlasst, eine Leerungsoperation einer FDB in dem mindestens einen zweiten Ringknoten (32) durchzuführen.

10. Verfahren nach Anspruch 9, ferner den folgenden Schritt umfassend:
Reagieren, wobei der mindestens eine zweite Ringknoten (32) in dem Ethernetring (51, 61) konfiguriert ist, um einen ERP nach einem anderen ERP-Protokollstandard durchzuführen, auf von dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) gesendeten Konfigurationsnachrichten, sodass Standardoperationen des ERP nach dem anderen ERP-Protokollstandard in dem mindestens einen zweiten Ringknoten (32) nicht gestört werden.

11. Verfahren nach Anspruch 10, ferner den folgenden Schritt umfassend:
Antworten, falls der andere ERP-Protokollstandard Rapid-Spanning-Tree-Protokoll (RSTP) ist, auf die Konfigurationsnachrichten, die von dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) während der Ersteinrichtung des RSTP gesendet werden.

12. Ethernetring (51, 61), umfassend einen ersten Ringknoten (53) nach Anspruch 1 und mindestens einen dritten Ringknoten (54), der zum Schutz gegen die Schleifen in dem Ethernetring (51, 61) durch Durchführen des ERP nach dem ERP-Protokollstandard eingerichtet ist, **dadurch gekennzeichnet, dass** der mindestens eine dritte Ringknoten (54), der sich unmittelbar benachbart zu dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) befindet, konfiguriert ist, um bei Erkennen des Verbindungsfehlerereignisses oder des Wiederherstellungsereignisses in dem Ethernetring (51, 61), das zu einer Leerungsoperation von FDB in dem mindestens einen dritten Ringknoten (54) nach dem ERP-Protokollstandard führt, eine Nachricht an den mindestens einen zweiten Ringknoten (32) zu senden, wobei die von dem mindestens einen dritten

Ringknoten (54) gesendete Nachricht so betreibbar ist, dass sie den mindestens einen zweiten Ringknoten (32) veranlasst, eine Leerungsoperation der FDB in dem mindestens einen zweiten Ringknoten (32) durchzuführen.

13. Ethernetring (51, 61) nach Anspruch 12, wobei, falls der mindestens eine zweite Ringknoten (32) konfiguriert ist, um einen ERP nach einem anderen ERP-Protokollstandard durchzuführen, und mehr als einen Ringknoten (D1, D2) umfasst, Resilienzmaßnahmen für eine Konnektivität zwischen den mehr als einem Ringknoten (D1, D2) bereitgestellt werden.

14. Breitbandkommunikationsnetz, umfassend einen ersten Ringknoten (53) nach Anspruch 1 und/oder einen Ethernetring (51, 61) nach Anspruch 12.

15. Verfahren zur Verwendung in einem Ethernetring (51, 61) nach Anspruch 9, wobei der Ethernetring (51, 61) ferner mindestens einen dritten Ringknoten (54) umfasst, der so eingerichtet ist, dass er gegen die Schleifen in dem Ethernetring (51, 61) schützt, indem er den ERP nach dem ERP-Protokollstandard durchführt, wobei das Verfahren die folgenden Schritte umfasst:
Entscheiden, eine Leerungsoperation einer FDB in dem mindestens einen dritten Ringknoten (54) als Reaktion auf das erkannte Verbindungsfehlerereignis oder das erkannte Wiederherstellungsereignis durchzuführen, wobei das Verfahren **dadurch gekennzeichnet ist, dass** es ferner den folgenden Schritt umfasst:
als Reaktion auf die Entscheidung, die Leerungsoperation der FDB in dem mindestens einen dritten Ringknoten (54) durchzuführen, Senden einer Nachricht von dem mindestens einen dritten Ringknoten (54), der sich unmittelbar benachbart zu dem mindestens einen zweiten Ringknoten (32) in dem Ethernetring (51, 61) befindet, an den mindestens einen zweiten Ringknoten (32), wobei die von dem mindestens einen dritten Ringknoten (54) gesendete Nachricht so betreibbar ist, dass sie den mindestens einen zweiten Ringknoten (32) veranlasst, eine Leerungsoperation der FDB in dem mindestens einen zweiten Ringknoten (32) durchzuführen.

Revendications

1. Premier nœud d'anneau (53) agencé pour protéger contre les boucles dans un anneau Ethernet (51, 61) en exécutant une protection d'anneau Ethernet, ERP, conformément à une norme de protocole ERP, le premier nœud d'anneau (53) étant situé directement adjacent à au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61), dans lequel l'au moins un deuxième nœud d'anneau (32) n'est pas configuré pour exécuter une ERP conformément à la même norme de protocole ERP, **caractérisé en ce que**
le premier nœud d'anneau (53) est configuré pour, lors d'une détection d'un événement de défaillance de liaison ou d'un événement de récupération dans l'anneau Ethernet (51, 61) entraînant une opération de vidage d'une base de données de filtrage, FDB, dans le premier nœud d'anneau (53) conformément à la norme de protocole ERP, envoyer un message à l'au moins un deuxième nœud d'anneau (32), dans lequel le message peut être utilisé pour amener ledit au moins un deuxième nœud d'anneau (32) à exécuter une opération de vidage d'une FDB dans l'au moins un deuxième nœud d'anneau (32).

2. Premier nœud d'anneau (53) selon la revendication 1, dans lequel le premier nœud d'anneau (53) est configuré pour être relié en communication avec un troisième nœud d'anneau (54) dans l'anneau Ethernet (51, 61) en tunnelisant un VLAN utilisé par la norme de protocole ERP à travers l'au moins un deuxième nœud d'anneau (32), dans lequel ledit troisième nœud d'anneau (54) dans l'anneau Ethernet (51, 61) est configuré pour exécuter une ERP conformément à la même norme de protocole ERP que le premier nœud d'anneau (53).

3. Premier nœud d'anneau (53) selon la revendication 1 ou 2, dans lequel l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) est configuré pour exécuter une ERP conformément à une autre norme de protocole ERP.

4. Premier nœud d'anneau (53) selon la revendication 3, dans lequel le premier nœud d'anneau (53) est en outre configuré pour réagir à des messages de configuration envoyés par l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) conformément à l'une autre norme de protocole ERP de sorte que des opérations de norme d'ERP, conformément à l'une autre norme de protocole ERP, dans l'au moins un deuxième nœud d'anneau (32) ne sont pas perturbées.

5. Premier nœud d'anneau (53) selon l'une quelconque des revendications 1 à 4, dans lequel la norme de protocole ERP pour le premier nœud d'anneau (53) est le protocole de commutation ERP ITU-T G.8032, et l'une autre norme de protocole ERP pour l'au moins un deuxième nœud d'anneau (32) est le protocole Spanning Tree Protocol, STP, ou le protocole Rapid Spanning Tree Protocol, RSTP.

6. Premier nœud d'anneau (53) selon la revendication 5, dans lequel, si l'une autre norme de protocole ERP est le RSTP, le premier nœud d'anneau (53) est en outre configuré pour répondre aux messages de configuration envoyés par l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) lors de la configuration initiale du RSTP.

7. Premier nœud d'anneau (53) selon l'une quelconque des revendications 5 à 6, dans lequel le message comprend une notification de changement de topologie de Spanning Tree Protocol, STP TCN, ou une notification de changement de topologie de Rapid Spanning Tree Protocol, RSTP TCN, et dans lequel le message est envoyé par le premier nœud d'anneau (53) à l'au moins un deuxième nœud d'anneau (32) à l'aide d'une interface réseau interne-réseau, I-NNI.

8. Premier nœud d'anneau (53) selon l'une quelconque des revendications 1 à 7, dans lequel les événements de défaillance de liaison ou les événements de récupération se produisant entre le premier nœud d'anneau (53) et l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) sont également supervisés par des messages de contrôle de continuité, CCM, Ethernet conformément au protocole de la norme de gestion des défauts de connectivité IEEE 802.1 ag.

9. Procédé à utiliser dans un premier nœud d'anneau (53) pour protéger contre les boucles dans un anneau Ethernet (51, 61) en exécutant une protection d'anneau Ethernet, ERP, conformément à une norme de protocole ERP, le premier nœud d'anneau (53) étant situé directement adjacent à au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61), dans lequel l'au moins un deuxième nœud d'anneau (32) n'est pas configuré pour exécuter une ERP conformément à la même norme de protocole ERP, le procédé comprenant les étapes de :

détection d'un événement de défaillance de liaison ou d'un événement de récupération dans l'anneau Ethernet (51, 61) conformément à la norme de protocole ERP ;
décision d'exécuter une opération de vidage d'une base de données de filtrage, FDB, dans le premier nœud d'anneau (53) en réponse à l'événement de défaillance de liaison détecté ou à l'événement de récupération détecté, ledit procédé étant **caractérisé en ce qu'**il comprend en outre l'étape :
en réponse à la décision d'exécuter l'opération de vidage, d'envoi d'un message à l'au moins un deuxième nœud d'anneau (32), dans lequel le message peut être utilisé pour amener ledit au moins un deuxième nœud d'anneau (32) à exécuter une opération de vidage d'une FDB dans l'au moins un deuxième nœud d'anneau (32) .

10. Procédé selon la revendication 9, comprenant en outre l'étape de :
réaction, dans lequel l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) est configuré pour exécuter une ERP conformément à une autre norme de protocole ERP, à des messages de configuration envoyés par l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) de sorte que des opérations de norme d'ERP, conformément à l'une autre norme de protocole ERP, dans l'au moins un deuxième nœud d'anneau (32) ne sont pas perturbées.

11. Procédé selon la revendication 10, comprenant en outre l'étape de :
réponse, si l'une autre norme de protocole ERP est Rapid Spanning Tree Protocol, RSTP, aux messages de configuration envoyés par l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) lors de la configuration initiale du RSTP.

12. Anneau Ethernet (51, 61) comprenant un premier nœud d'anneau (53) selon la revendication 1 et au moins un troisième nœud d'anneau (54) agencé pour protéger contre lesdites boucles dans l'anneau Ethernet (51, 61) en exécutant ladite ERP conformément à ladite norme de protocole ERP, **caractérisé en ce que**
l'au moins un troisième nœud d'anneau (54) qui est situé directement adjacent à l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) est configuré pour, lors de la détection de l'événement de défaillance de liaison ou de l'événement de récupération dans l'anneau Ethernet (51, 61) entraînant une opération de vidage de FDB dans l'au moins un troisième nœud d'anneau (54) conformément à la norme de protocole ERP, envoyer un message audit au moins un deuxième nœud d'anneau (32), dans lequel le message envoyé par l'au moins un troisième nœud d'anneau (54) peut être utilisé pour amener ledit au moins un deuxième nœud d'anneau (32) à exécuter une opération de vidage de la FDB dans l'au moins un deuxième nœud d'anneau (32).

13. Anneau Ethernet (51,61) selon la revendication 12, dans lequel, si l'au moins un deuxième nœud d'anneau (32) est configuré pour exécuter une ERP conformément à une autre norme de protocole ERP et comprend plusieurs nœuds d'anneau (D1, D2), des mesures de résilience pour une connectivité entre les plusieurs nœuds d'anneau (D1, D2) sont prévues.

14. Réseau de communications à large bande comprenant un premier nœud d'anneau (53) selon la revendication 1, et/ou un anneau Ethernet (51, 61) selon la revendication 12.

15. Procédé, à utiliser dans un anneau Ethernet (51, 61) selon la revendication 9, l'anneau Ethernet (51, 61) comprenant en outre au moins un troisième nœud d'anneau (54) agencé pour protéger contre lesdites boucles dans l'anneau Ethernet (51, 61) en exécutant ladite ERP conformément à ladite norme de protocole ERP, le procédé comprenant les étapes de : décision d'exécuter une opération de vidage d'une FDB dans l'au moins un troisième nœud d'anneau (54) en réponse à l'événement de défaillance de liaison détecté ou à l'événement de récupération détecté, le procédé étant **caractérisé en ce qu'**il comprend en outre l'étape :
en réponse à la décision d'exécuter l'opération de vidage de ladite FDB dans ledit au moins un troisième nœud d'anneau (54), d'envoi d'un message, depuis l'au moins un troisième nœud d'anneau (54) qui est situé directement adjacent à l'au moins un deuxième nœud d'anneau (32) dans l'anneau Ethernet (51, 61) à l'au moins un deuxième nœud d'anneau (32), dans lequel le message envoyé par ledit au moins un troisième nœud d'anneau (54) peut être utilisé pour amener ledit au moins un deuxième nœud d'anneau (32) à exécuter une opération de vidage de ladite FDB dans l'au moins un deuxième nœud d'anneau (32).

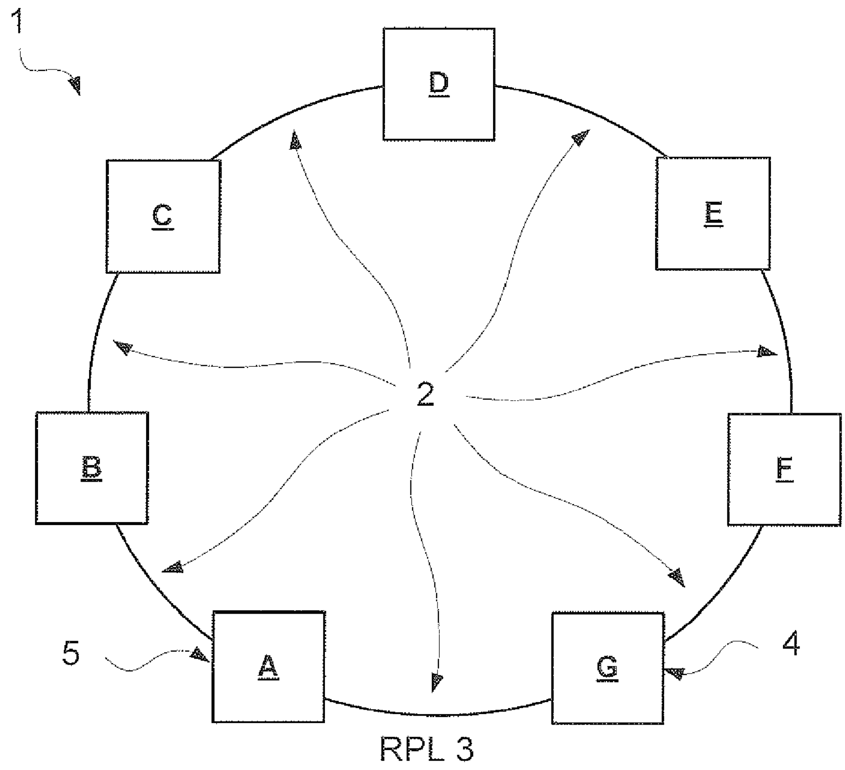

Fig. 1 - PRIOR ART

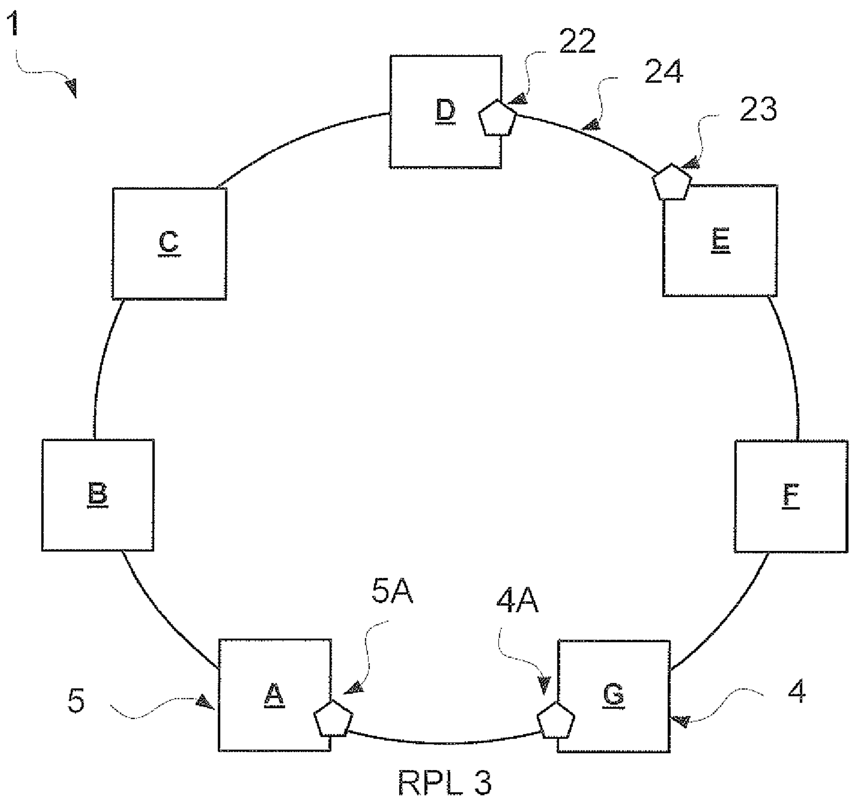

Fig. 2 - PRIOR ART

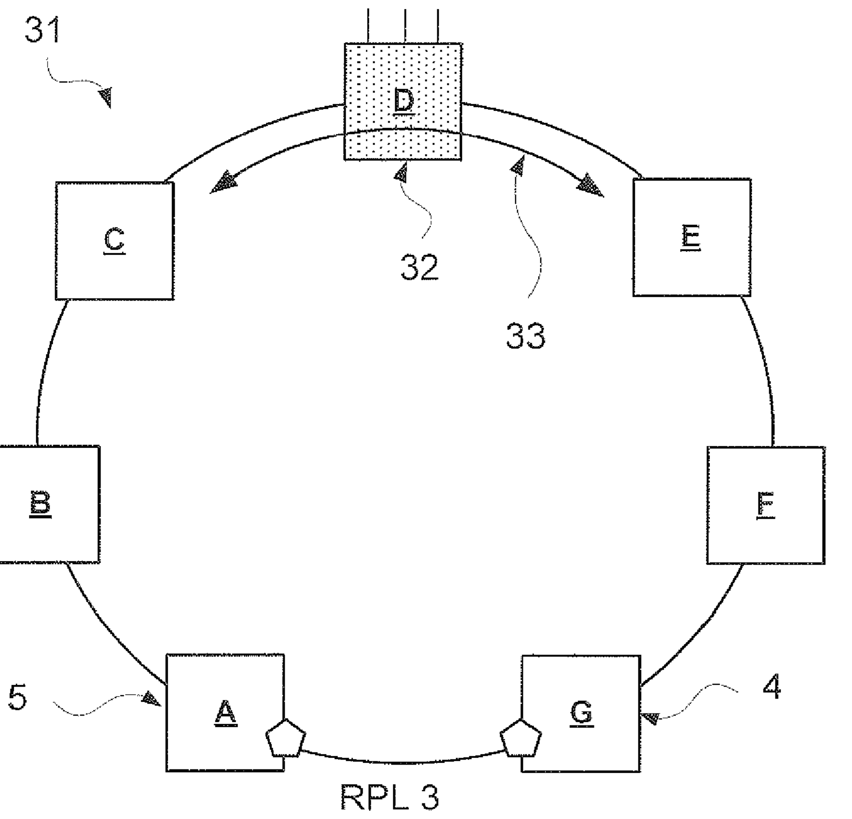

Fig. 3

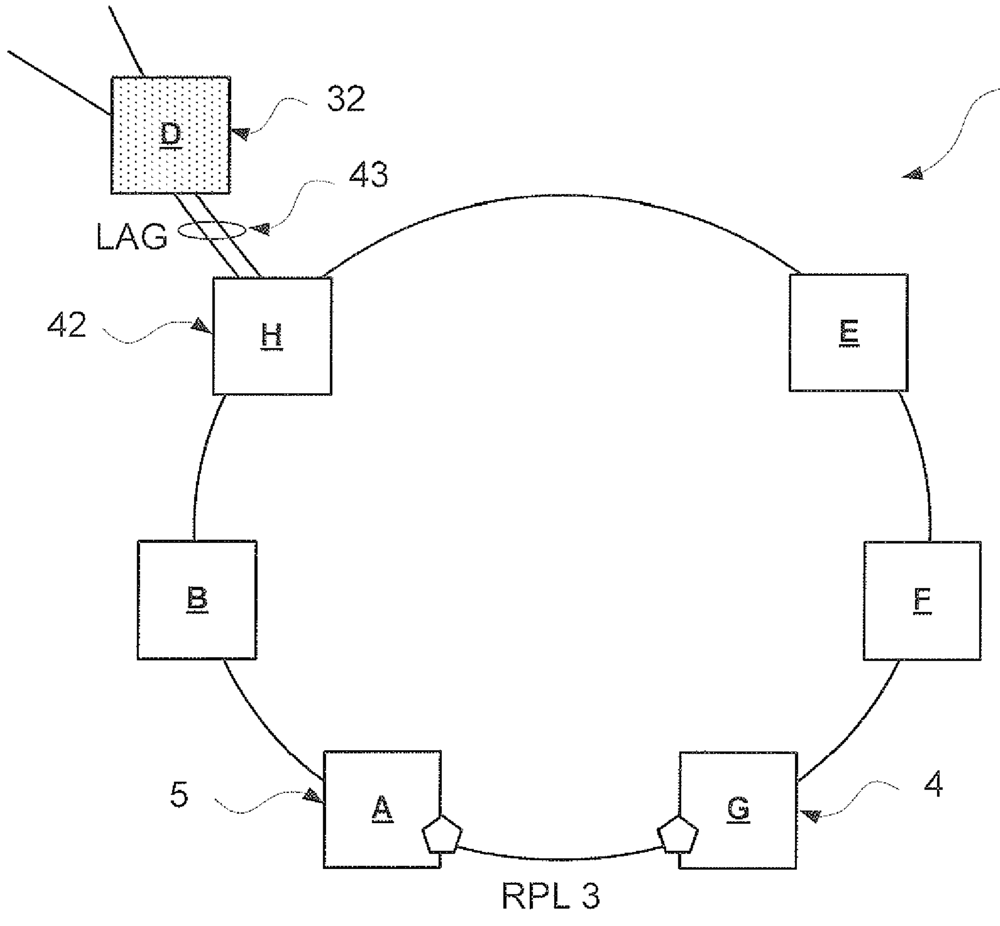

Fig. 4

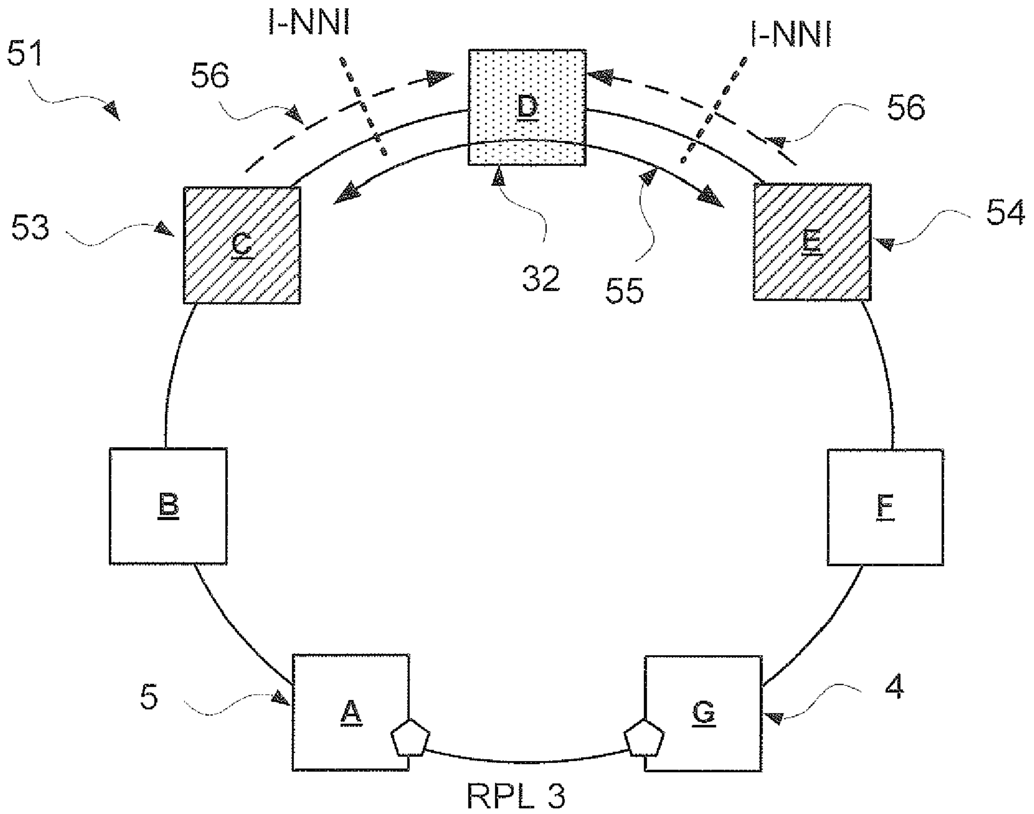
51
56
I-NNI
D
I-NNI
56
53
C
32
55
E
54
B
F
5
A
G
4
RPL 3

Fig. 5

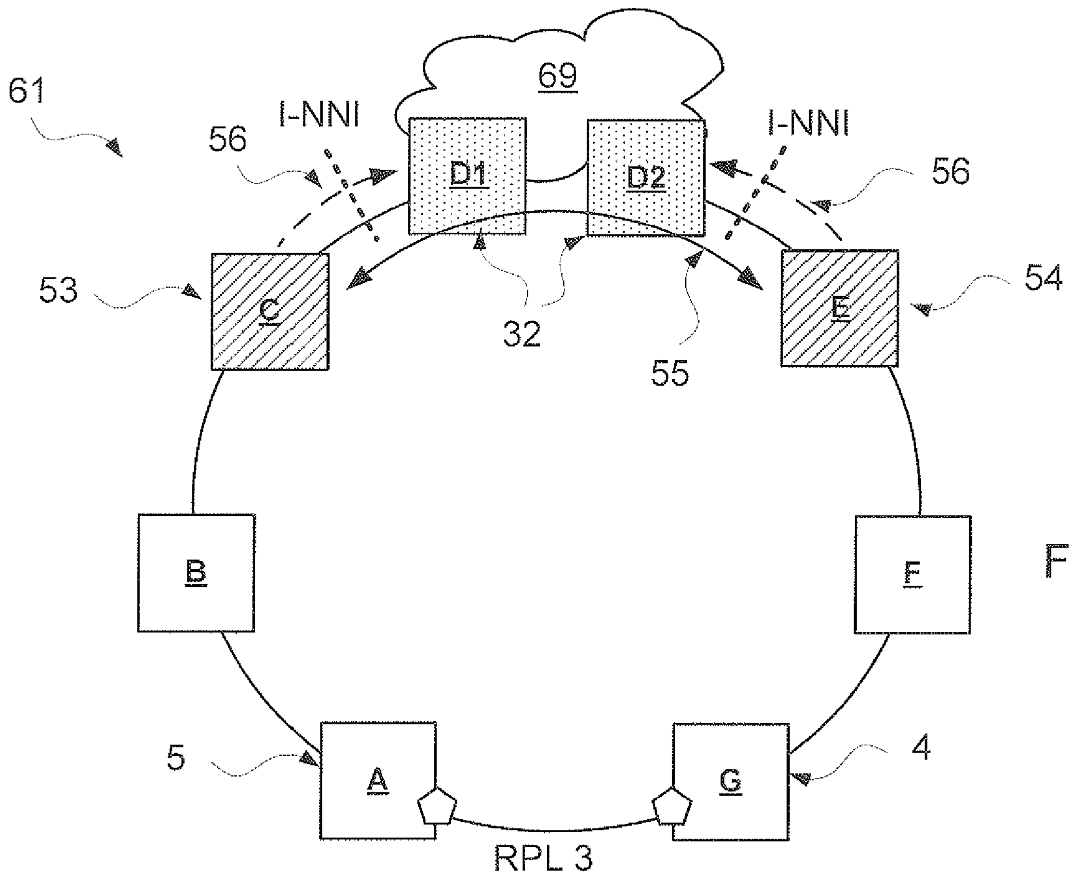
61
69
56
I-NNI
D1
D2
I-NNI
56
53
C
32
55
E
54
B
F
5
A
G
4
RPL 3

Fig. 6

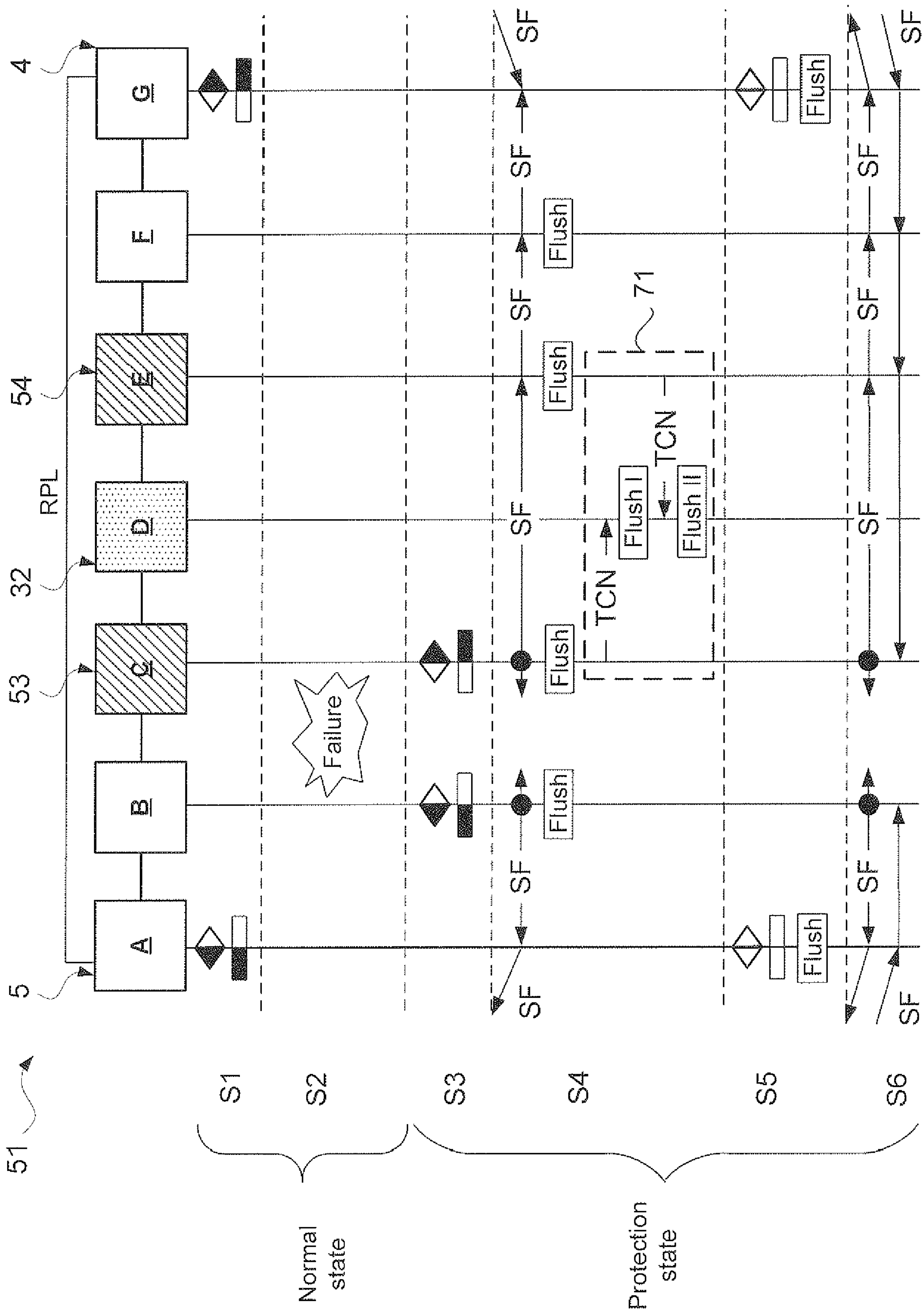
51
5
53
32
54
4
RPL
A
B
C
D
E
F
G
Failure
S1
S2
S3
S4
S5
S6
SF
Flush
TCN
Flush I
Flush II
71
Normal state
Protection state

Fig. 7

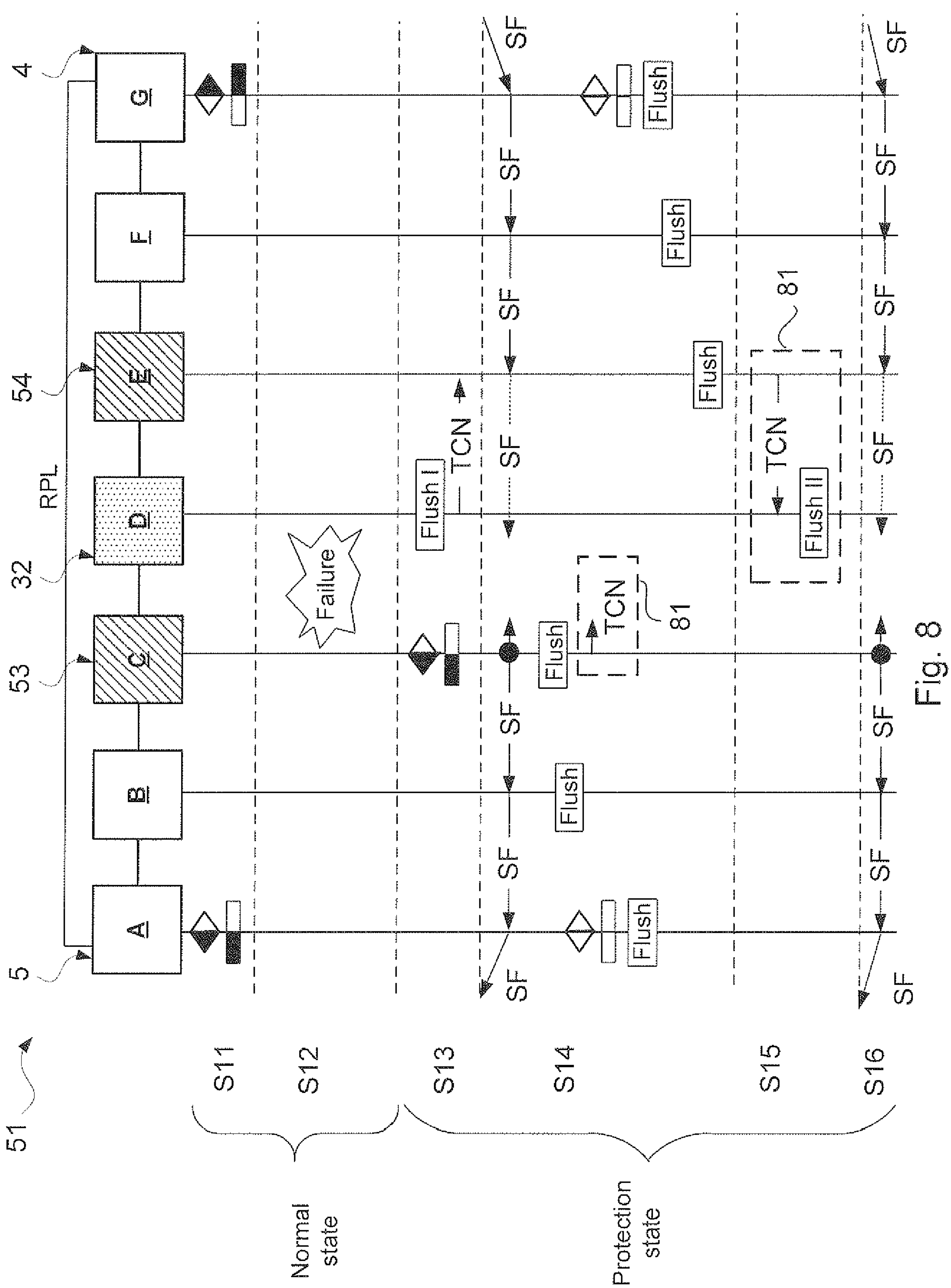
51
5
53
32
54
4
RPL
A
B
C
D
E
F
G
Failure
Flush I
TCN
Flush
Flush II
81
SF
S11
S12
S13
S14
S15
S16
Normal state
Protection state

Fig. 8

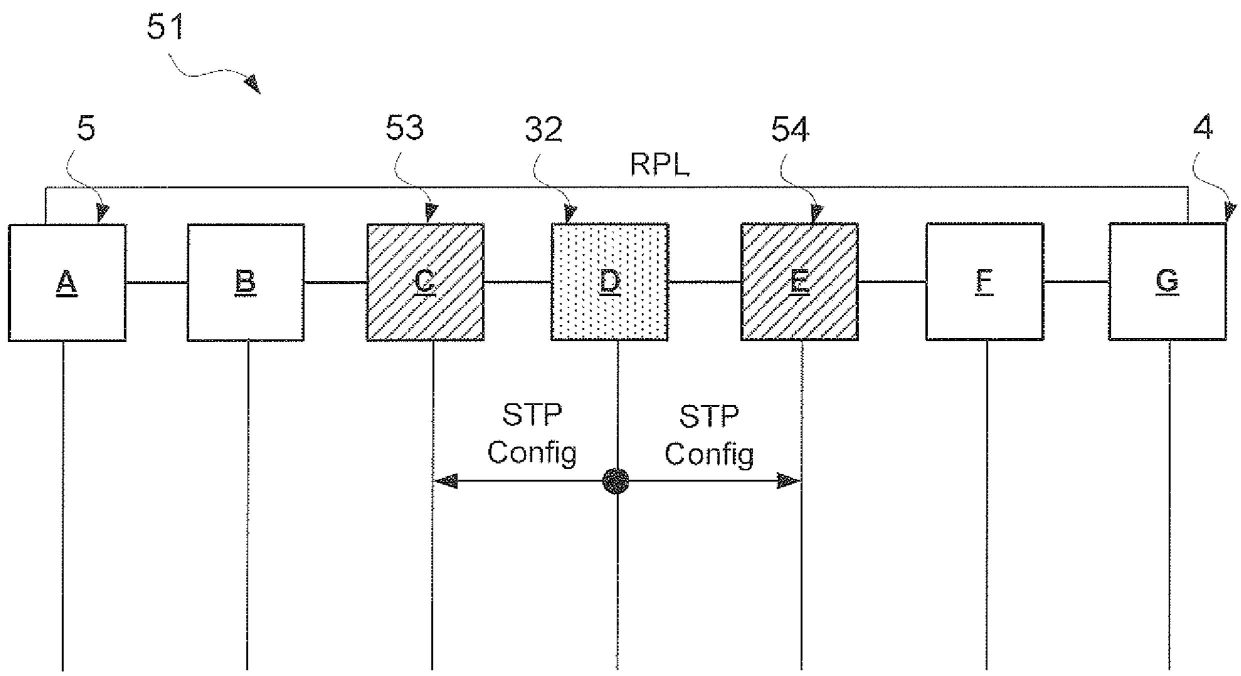
51
5
53
32
54
4
RPL
A
B
C
D
E
F
G
STP Config
STP Config

Fig. 9

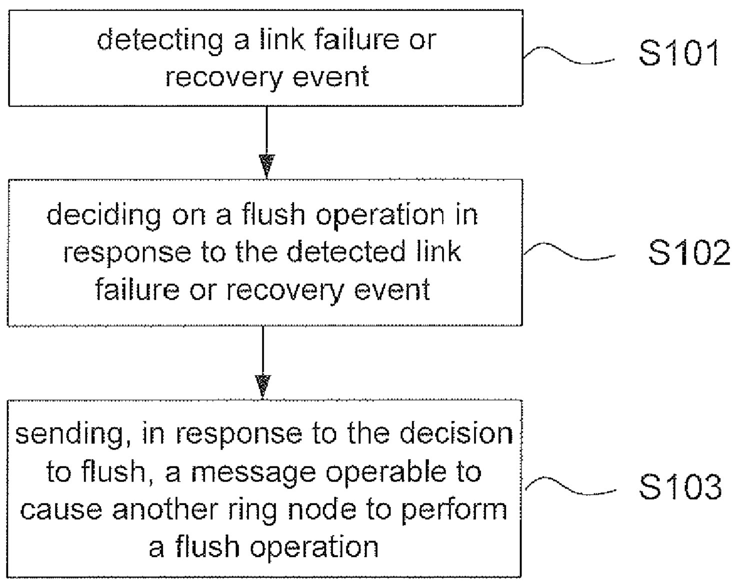
detecting a link failure or recovery event
S101
deciding on a flush operation in response to the detected link failure or recovery event
S102
sending, in response to the decision to flush, a message operable to cause another ring node to perform a flush operation
S103

Fig. 10

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2009168647 A **[0009]**